Docket No. 212288US2S

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Fumihikko SANO
GAU:
SERIAL NO: NEW APPLICATION
EXAMINER:
FILED: HEREWITH
FOR: ENCRYPTION/DECRYPTION APPARATUS, AUTHENTICATING APPARATUS, PROGRAM AND METHOD

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-237268	August 4, 2000

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913
C. Irvin McClelland
Registration Number 21,124

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日 本 国 特 許 庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　８月　４日

出願番号
Application Number: 特願２０００－２３７２６８

出願人
Applicant(s): 株式会社東芝

２００１年　６月２７日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０６０４９６

【書類名】　特許願

【整理番号】　A009904721

【提出日】　平成12年 8月 4日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 9/00

【発明の名称】　暗復号装置、認証装置及び記憶媒体

【請求項の数】　8

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中事業所内

【氏名】　佐野　文彦

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗復号装置、認証装置及び記憶媒体

【特許請求の範囲】

【請求項１】　互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部と、

いずれかの暗号化関数部の中間的な処理結果に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段とを備えた暗復号装置であって、

前記各鍵データ生成手段は、互いに異なる２つ以上の変換処理のうち、いずれかの変換処理を用いて前記共通鍵を変換することを特徴とする暗復号装置。

【請求項２】　請求項１に記載の暗復号装置において、

前記各鍵データ生成手段は、互いに異なる２つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とする暗復号装置。

【請求項３】　メッセージから認証子を生成する認証子生成手段を備え、前記認証子生成手段により生成された認証子に基づいて前記メッセージの認証を行なう認証装置であって、

前記認証子生成手段は、

互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部と、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる２つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部と、

最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子を作成する認証子作成部と

を備えたことを特徴とする認証装置。

【請求項４】　請求項３に記載の認証装置において、

前記各鍵データ生成部は、互いに異なる２つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とする認証装置。

【請求項５】　暗復号装置のコンピュータを、

互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる２つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段、

として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項６】　請求項５に記載のコンピュータ読取り可能な記憶媒体において、

前記各鍵データ生成手段は、互いに異なる２つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とするコンピュータ読取り可能な記憶媒体。

【請求項７】　メッセージから認証子を生成し、この認証子に基づいて前記メッセージの認証を行なう認証装置に使用されるコンピュータ読取り可能な記憶媒体であって、

前記認証装置のコンピュータを、

互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる２つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部、

最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子

を作成する認証子作成部、

として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項８】　請求項７に記載のコンピュータ読取り可能な記憶媒体において、

前記各鍵データ生成部は、互いに異なる２つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とするコンピュータ読取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ブロック暗号における暗号化連鎖方式を用いた暗復号装置、認証装置及び記憶媒体に係り、特に、各ブロック間での連鎖のさせ方を全体で２種類以上設けて安全性を向上し得る暗復号装置、認証装置及び記憶媒体に関する。

【０００２】

【従来の技術】

近年、計算機や通信技術の分野では、送信データを暗号化して送信し、受信データを復号して受信内容を得る暗号技術が広く知られている。この種の暗号技術では、暗号化と復号に同じ秘密鍵（以下、共通鍵という）を用いる暗号化アルゴリズムが共通鍵暗号方式と呼ばれている。共通鍵暗号方式では、一般に、入力される平文データが固定長の入力ブロックに分割され、各ブロックが共通鍵から生成される鍵に基づいて攪拌処理され、暗号文に変換されている。

【０００３】

ここで、平文データが暗号化アルゴリズムのブロック長よりも長い場合、入力データがブロック長で分割され、暗号化された結果がＣＢＣモード（cipher block chaining mode；暗号文連鎖モード）、インナーＣＢＣモード（inner ＣＢＣ mode）、ＣＢＣＭモード（ＣＢＣ message mode）といった周知の暗号化連鎖方式により、結合される。

【０００４】

図７はこの種の暗号化連鎖方式の適用された暗復号装置の構成を示す模式図である。この暗復号装置では、入力された平文データが一定長のｍ個の平文ブロックＰ１～Ｐｍに分割され、各平文ブロックＰ１～Ｐｍが、互いに並列配置されたｍ個の暗号化関数Ｆ１～Ｆｍのいずれかに入力される。各暗号化関数Ｆ１～Ｆｍは、入力された平文ブロックＰ１～Ｐｍを共通鍵Ｋに基づく鍵データにより暗号化し、それぞれ暗号文ブロックＣ１～Ｃｍに変換して出力する。なお、暗復号装置は、暗号文ブロックＣ１～Ｃｍが入力されると、この暗号文ブロックＣ１～Ｃｍを上記暗号化と逆の処理にて復号し、それぞれ平文ブロックＰ１～Ｐｍに変換して出力する。

【０００５】

ここで、１番目の暗号化関数Ｆ１は、１番目の平文ブロックＰ１と共通鍵Ｋが入力されると、１番目の中間出力i_1を１番目の変換関数f_1に入力する一方、暗号文Ｃ１を出力する。

【０００６】

１番目の変換関数f_1は、例えば非線形な関数が用いられ、暗号化関数Ｆ１の中間出力i_1を変換し、得られた変換結果s_1を１番目の変換関数g_1に入力する。なお、２番目～(m-1)番目の変換関数f_2～f_{m-1}も同様である。

【０００７】

１番目の変換関数g_1は、例えば排他的論理和又は加算といった線形関数が用いられ、別途入力された共通鍵Ｋを、変換関数f_1の変換結果s_1により変換し、得られた変換結果Ｋｇ２を２番目の暗号化関数Ｆ２に入力する。また、２番目～(m-1)番目の変換関数g_2～g_{m-1}も同様である。

【０００８】

以下同様に、共通鍵Ｋは、(n-1)番目の暗号化関数Ｆ(n-1)による中間出力i_{n-1}と、(n-1)番目の変換関数f_{n-1}，g_{n-1}とに基づいて、鍵データＫｇｎ（但し２≦ｎ≦ｍ）に変換され、鍵データＫｇｎとしてｎ番目の暗号化関数Ｆｎに入力される。係る前段の中間出力i_{n-1}と共通鍵Ｋから次段の鍵データＫｇｎを生成する処理は、ｍ番目の暗号化関数Ｆｍに鍵データＫｇｍを入力するまで行なわれる。なお、各変換関数g_1～g_{m-1}に入力される共通鍵Ｋは、１番目の暗号化関数

Ｆ１に入力された共通鍵Ｋと同一である。

【０００９】

係る暗号化連鎖方式では、ｍ個の暗号化関数Ｆ１～Ｆｍに使用される鍵Ｋ，Ｋｇ２～Ｋｇｍが互いに異なるため、高い安全性を有している。

しかしながら、以上のような暗号化連鎖方式では、互いに同一の平文ブロックＰ１～Ｐｍが入力された場合、全ての変換関数f_1～f_{m-1}の変換結果s_1～s_{m-1}が０となり、共通鍵Ｋを変換関数g_1～g_{m-1}で変換した変換結果Ｋｇ２～Ｋｇｍと、共通鍵Ｋとが一致してしまう。

【００１０】

なお、各鍵Ｋ，Ｋｇ２～Ｋｇｍが一致した場合、ｍ個の暗号化関数Ｆ１～Ｆｍにて同一の暗号化が実行され、同一のｍ個の暗号文ブロックＣ１，Ｃ２，Ｃ３，…，Ｃｍが出力される。この現象は、暗号解読の大きな手がかりとなり、暗号解読手法に対する安全性を低下させてしまう。

【００１１】

【発明が解決しようとする課題】

以上説明したように従来の暗号化連鎖方式を用いた暗復号装置では、特定パターンの平文ブロックＰ１～Ｐｍの入力により、全ての変換関数f_1～f_{m-1}の出力が０となって共通鍵Ｋが変換されない場合がある。これを阻止するには、変換関数f_1～f_{m-1}の出力が０にならないよう、平文ブロックＰ１～Ｐｍや鍵Ｋｇ２～Ｋｇｍを注意深く検査する必要がある。

【００１２】

係る検査は、特定パターンをもつ平文ブロックＰ１～Ｐｍの入力を除去する装置などを付加すれば実現可能である。しかしながら、この種の除去装置を付加する解決手法では、暗号化連鎖方式の価格を上昇させると共に、暗号化連鎖方式の規模を増大させてしまう問題が生じる。

【００１３】

また、係る除去装置は、暗号強度の向上には寄与しない。すなわち、費用対効果の観点からは、暗号強度を向上し得る他の解決手法が望まれている。

【００１４】

本発明は上記実情を考慮してなされたもので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上し得る暗復号装置、認証装置及び記憶媒体を提供することを目的とする。

【００１５】

【課題を解決するための手段】

第１の発明は、互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部と、いずれかの暗号化関数部の中間的な処理結果に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段とを備えた暗復号装置であって、前記各鍵データ生成手段としては、互いに異なる２つ以上の変換処理のうち、いずれかの変換処理を用いて前記共通鍵を変換する暗復号装置である。

【００１６】

また、第２の発明は、メッセージから認証子を生成する認証子生成手段を備え、前記認証子生成手段により生成された認証子に基づいて前記メッセージの認証を行なう認証装置であって、前記認証子生成手段としては、互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部と、いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる２つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部と、最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子を作成する認証子作成部とを備えた認証装置である。

【００１７】

ここで、第１の発明における各鍵生成手段、及び／又は第２の発明における各データ生成部は、互いに異なる２つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換する構成としてもよい。

【００１８】

また、第１及び第２の発明は、前述した機能を記述したプログラムを記憶したコンピュータ読取り可能な記憶媒体を用い、当該記憶媒体をコンピュータにインストールして実現させてもよい。

【００１９】

（作用）

従って、第１の発明は以上のような手段を講じたことにより、暗号化連鎖方式に用いられる各鍵データ生成手段が、互いに異なる２つ以上の変換処理のうち、いずれかの変換処理を用いて共通鍵を変換する。

【００２０】

これにより、共通鍵の変換結果である鍵データが平文データから一義的には決まらなくなるので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

【００２１】

また、第２の発明は、認証子を作成する際に、第１の発明の暗復号装置を用いるので、第１の発明の作用を奏する認証技術を実現させることができる。

【００２２】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。

（第１の実施形態）

図１は本発明の第１の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図であり、図７と同種の要素には同一符号を付してその詳しい説明を省略し、ここでは異なる要素について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

すなわち、本実施形態は、互いに同一の平文ブロックＰ１～Ｐｍが入力されても、異なる鍵データＫｇ２～Ｋｇｍを生成させ、安全性の向上を図るものであって、具体的には、各変換関数g_1～g_{m-1}に個別に変数v_1～v_{m-1}を入力するための変数入力部V_1～V_{m-1}を設けている。

【００２３】

ここで、(m-1)個の変数入力部V_1～V_{m-1}は、それぞれ変数v_1～v_{m-1}を個

別に変換関数g_1～g_{m-1}に入力する機能をもっている。

各変数v_1～v_{m-1}は、全体として２種類以上～(m-1)種類以下の範囲で異なる値が設定可能であり、全体として種類が多いほど、攪拌性向上の観点から好ましい。各変数v_1～v_{m-1}は、例えば図２に示すように、初期値（例、システム固有の値）ＩＶをレジスタに格納し、同一の変換関数で順次変換することにより、生成可能となっている。

また、変数v_1～v_{m-1}の種類が例えば３種類の場合、v_1～$v_{(m-1)/3}$が第１の値、$v_{\{(m-1)/3\}+1}$～$v_{(m-1)\cdot 2/3}$が第２の値、$v_{\{(m-1)\cdot 2/3\}+1}$～v_{m-1}が第３の値という設定よりも、v_1が第１の値、v_2が第２の値、v_3が第３の値、v_4が第１の値、…という設定の方が攪拌性向上の観点から好ましい。すなわち、各変数v_1～v_{m-1}は、ｔ種類の値を取り得る場合、互いに隣接する任意のｔ個の変数（例、v_1～v_t，v_2～v_{t+1}，…，v_{m-t}～v_{m-1}）を互いに異なる値とする設定の方が好ましい。

【００２４】

なお、各変換関数g_1～g_{m-1}は、変数入力部V_1～V_{m-1}から入力された変数v_1～v_{m-1}と変換関数f_1～f_{m-1}から入力された変換結果s_1～s_{m-1}とに基づいて、別途入力された共通鍵Ｋを変換し、得られた変換結果Ｋｇ２～Ｋｇｍを次段の暗号化関数Ｆ２～Ｆｍに入力する機能をもっている。なお、各変換関数g_1～g_{m-1}における変換機能としては、前述した通り、例えば排他的論理和又は加算の如き、線形関数が用いられている。

【００２５】

また、変換関数f_1～f_{m-1}は、例えば次の変換処理（１）～（８）のうち、任意の１種類の変換処理が使用されている。

（１）入力から任意のビット長を切り落として出力するビット切落し処理。

（２）入力のビット長を必要なビット長とするまでダミービットを埋込むパディング処理。なお、ダミービットは、ブランクなどの冗字や０などが使用可能である。

（３）入力のビットを反転させて出力するビット反転処理。

（４）入力のビットを逆順に並べ換えて出力するビット逆順処理。

（５）入力のビット同士を任意に置換して出力するビット置換処理。

（６）入力をハッシュ関数で変換したものから任意のビット長を切り落として出力するハッシュ関数（例、ＳＨＡ－１，ＭＤ５等）＋ビット切落し処理。

（７）入力に定数を加算して出力する定数加算処理。

（８）入力を恒等変換して出力する恒等変換処理。

【００２６】

また、係る暗復号装置は、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。

【００２７】

次に、以上のように構成された暗復号装置の動作を説明する。

いま、暗復号装置では、前述同様に、入力された平文データが一定長のｍ個の平文ブロックＰ１～Ｐｍに分割され、各平文ブロックＰ１～Ｐｍが、互いに並列配置されたｍ個の暗号化関数Ｆ１～Ｆｍのいずれかに入力される。

【００２８】

また、各暗号化関数Ｆ１～Ｆｍは、入力された平文ブロックＰ１～Ｐｍを共通鍵Ｋに基づく鍵データにより暗号化し、それぞれ暗号文ブロックＣ１～Ｃｍに変換して出力する。

【００２９】

例えば１番目の暗号化関数Ｆ１は、１番目の平文ブロックＰ１と共通鍵Ｋが入力されると、１番目の中間出力i_1を１番目の変換関数f_1に入力する一方、暗号文Ｃ１を出力する。

【００３０】

１番目の変換関数f_1は、暗号化関数Ｆ１の中間出力i_1を変換し、得られた変換結果s_1を１番目の変換関数g_1に入力する。

ここまでの過程は、鍵データの生成に関し、従来と同様である。

次に、本実施形態では、従来とは異なり、１番目の変数入力部V_1が１番目の変数v_1を１番目の変換関数g_1に入力する。

【００３１】

これにより、１番目の変換関数g_1は、変数入力部V_1からの変数v_1と変換関数f_1からの変換結果s_1とに基づいて、別途入力された共通鍵Ｋを変換し、得られた変換結果Ｋｇ２を次段の暗号化関数Ｆ２に入力する。

【００３２】

従って、１番目の暗号化関数Ｆ１の中間出力i_1が０であり、これに伴い、１番目の変換関数f_1の変換結果s_1が０であったとしても、１番目の変換関数g_1への入力は０にならず、変数v_1となる。

【００３３】

すなわち、１番目の変換関数f_1の変換結果s_1が０であっても、１番目の変換関数g_1から出力される鍵データＫｇ２は、共通鍵Ｋが変数v_1により変換された値となって次段の暗号化関数Ｆ２に入力される。

【００３４】

以下同様に、共通鍵Ｋは、(n-1)番目の暗号化関数Ｆ(n-1)による中間出力i_{n-1}と、(n-1)番目の変数入力部V_{n-1}による変数v_{n-1}と、(n-1)番目の変換関数f_{n-1}，g_{n-1}とに基づいて、鍵データＫｇｎに変換され、鍵データＫｇｎとしてｎ番目の暗号化関数Ｆｎに入力される。

【００３５】

係る前段の中間出力i_{n-1}と、前段の変数v_{n-1}と、共通鍵Ｋとから次段の鍵データＫｇｎを生成する処理は、ｍ番目の暗号化関数Ｆｍに鍵データＫｇｍを入力するまで行なわれる。

【００３６】

ここで、鍵データＫｇ２～Ｋｇｍは、平文ブロックＰ１～Ｐｍや中間結果i_1～i_{m-1}とは独立に入力される変数v_1～v_{m-1}に基づき、共通鍵Ｋが変換されたものである。このため、暗復号装置は、平文ブロックＰ１～Ｐｍの各ブロックを互いに同一データとして入力する暗号解読手法に攻撃されても、鍵データＫｇ２～Ｋｇｍを互いに異なる値に作成するので、安全性の低下を阻止することができる。

上述したように本実施形態によれば、暗号化連鎖方式において、鍵データＫｇ２～Ｋｇｍの生成の際に、不確定要素として変数v_1～v_{m-1}を入力することに

より、鍵データＫｇ２～Ｋｇｍを平文ブロックＰ１～Ｐｍから一義的には決まらないようにしたので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

また、ある暗号化関数Ｆｊに鍵データＫｇｊとして弱鍵(week key)、双対鍵(dual key)又はやや弱い鍵(semi-week key)が入力された場合であっても、以後の暗号化関数Ｆ(j+1)～Ｆ(m-1)には弱鍵とは異なる鍵データＫｇ(j+1)～Ｋｇ(m-1)が入力されるので、安全性を向上させることができる。

【００３７】

（第２の実施形態）

図３は本発明の第２の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図である。

すなわち、本実施形態は、第１の実施形態の変形例であり、具体的には、各変数入力部V_1～V_{m-1}に代えて、各変換関数f_1'～f_{m-1}'が、互いに異なる２以上の変換関数のいずれかとして構成されている。

【００３８】

ここで、互いに異なる変換関数（変換処理）とは、（ａ）違う関数を用いる場合と、（ｂ）同じ関数を異なるビット位置に作用させる場合（例、ビットの置換関数）と、（ｃ）同じ関数を異なる定数で作用させる場合（例、加算関数で加える定数）と、のいずれかの場合又はこれらを組合せた場合が適用可能となっている。なお、第１の実施形態は、変換関数g_1～g_{m-1}に対し、上記（ｃ）により異なる変換関数（変換処理）g_1～g_{m-1}とした例に該当する。

【００３９】

また、各変換関数f_1'～f_{m-1}'は、例えば前述した変換処理（１）～（８）のうち、任意の１種類以上の変換処理が使用可能となっている。

【００４０】

なお、各変換関数f_1'～f_{m-1}'は、ｔ種類の異なる関数が適用される場合、互いに隣接する任意のｔ個の変換関数（例、f_1'～f_t'，f_2'～f_{t+1}'，…，f_{m-t}'～f_{m-1}'）を互いに異なる関数とする設定の方が好ましい。

【００４１】

以上のような構成としても、第１の実施形態と同様に、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

また同様に、ある暗号化関数Ｆｊに鍵データＫｇｊとして弱鍵などが入力された場合でも、以後の暗号化関数Ｆ(j+1)～Ｆ(m-1)には弱鍵とは異なる鍵データＫｇ(j+1)～Ｋｇ(m-1)が入力されるので、安全性を向上させることができる。

【００４２】

（第３の実施形態）

図４は本発明の第３の実施形態に係る認証方式の適用された第１及び第２のエンティティ装置の構成を示す模式図であり、図５は各エンティティ装置に用いられるＭＡＣ計算部の構成を代表して示す模式図である。

【００４３】

すなわち、本実施形態は、第１の実施形態の暗復号装置をＭＡＣ計算部に用いた認証方式を示し、第１及び第２のエンティティ装置１０Ａ，２０Ｂを備えている。

【００４４】

ここで、第１のエンティティ装置１０Ａは、メッセージ送信部１１Ａ、共通鍵記憶部１２Ａ、ＭＡＣ計算部１３Ａ及びＭＡＣ送信部１４Ａを備えている。

【００４５】

メッセージ送信部１１Ａは、メッセージＭを第２のエンティティ装置２０Ｂに送信する機能と、自己のＭＡＣ計算部１３Ａに送出する機能とをもっている。

【００４６】

共通鍵記憶部１２Ａは、第１及び第２のエンティティ装置１０Ａ，２０Ｂの両者で共有された共通鍵Ｋが記憶される領域であり、ＭＡＣ計算部１３Ａから読出可能となっている。

【００４７】

ＭＡＣ計算部１３Ａは、共通鍵記憶部１２Ａ内の共通鍵Ｋ及びメッセージ送信部１１Ａからのメッセージに基づいて、第１のＭＡＣ認証子＃１を算出（作成）する機能と、この第１のＭＡＣ認証子＃１をＭＡＣ送信部１４Ａに送出する機

能とをもっている。

【００４８】

ＭＡＣ送信部１４Ａは、ＭＡＣ計算部１３Ａから送出された第１のＭＡＣ認証子＃１を第２のエンティティ装置２０Ｂに送信する機能をもっている。

【００４９】

一方、第２のエンティティ装置２０Ｂは、メッセージ受信部２１Ｂ、共通鍵記憶部２２Ｂ、ＭＡＣ計算部２３Ｂ及び照合部２４Ｂを備えている。

メッセージ受信部２１Ｂは、第１のエンティティ装置１０Ａから送信されたメッセージＭを受信し、このメッセージＭを自己のＭＡＣ計算部２３Ｂに送出する機能をもっている。

【００５０】

共通鍵記憶部２２Ｂは、第１及び第２のエンティティ装置１０Ａ，２０Ｂの両者で共有された共通鍵Ｋが記憶される領域であり、ＭＡＣ計算部２３Ｂから読出可能となっている。

【００５１】

ＭＡＣ計算部２３Ｂは、共通鍵記憶部２２Ｂ内の共通鍵Ｋ及びメッセージ受信部２１Ｂからのメッセージに基づいて、第２のＭＡＣ認証子＃２を算出（作成）する機能と、この第２のＭＡＣ認証子＃２を照合部２４Ｂに送出する機能とをもっている。

【００５２】

照合部２４Ｂは、自己のＭＡＣ計算部２３Ｂから送出された第２のＭＡＣ認証子＃２と、第１のエンティティ装置１０Ａから受信した第１のＭＡＣ認証子＃１とを比較照合する機能と、両認証子＃１，＃２が一致するときに、第１のエンティティ装置１０Ａにより作成されたメッセージＭが改竄されずにメッセージ受信部２１Ｂに受信された旨を認証する機能と、両認証子＃１，＃２が不一致のときに、第１のエンティティ装置１０Ａにより作成されたメッセージＭが改竄された旨を検出する機能とをもっている。

【００５３】

続いて、第１及び第２のエンティティ装置１０Ａ，２０Ｂにおける各ＭＡＣ計

算部１３Ａ，２３Ｂの構成について説明する。なお、係るＭＡＣ計算部１３Ａ，２３Ｂは、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。また、両ＭＡＣ計算部１３Ａ，２３Ｂは互いに同一構成なので、ここでは第１のエンティティ装置１０Ａ内のＭＡＣ計算部１３Ａを例に挙げて述べる。

【００５４】

ＭＡＣ計算部１３Ａは、図５に示すように、図１に示した暗復号装置に対し、メッセージＭが平文データとして入力された際に、第１の実施形態で述べた通りに得られるｍ個目（最終）の暗号文ブロックＣｍのうち、所定ビット位置のデータを選択するビット選択部Ｂｓが付加された構成となっている。

【００５５】

なお、ビット選択部Ｂｓは、選択したデータを第１のＭＡＣ認証子＃１としてＭＡＣ送信部１４Ａに送出する機能をもっている。また、メッセージＭ自体は、平文データに限らず、図１の暗復号装置と同じ又は別の暗号化装置により暗号化された暗号文データであっても良い。

【００５６】

また、以上のような第１及び第２のエンティティ装置１０Ａ，２０Ｂは、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。

【００５７】

次に、以上のように構成された第１及び第２のエンティティ装置１０Ａ，２０Ｂの動作を説明する。

第１のエンティティ装置１０Ａは、メッセージ送信部１１ＡがメッセージＭを第２のエンティティ装置２０Ｂに送出すると共に、このメッセージＭと共通鍵Ｋとに基づき、ＭＡＣ計算部１３Ａが第１のＭＡＣ認証子＃１を算出し、ＭＡＣ送信部１４Ａがこの第１のＭＡＣ認証子＃１を第２のエンティティ装置２０Ｂに送信する。

【００５８】

第２のエンティティ装置２０Ｂは、第１のエンティティ装置１０ＡからメッセージM並びに第１のＭＡＣ認証子＃１を受信すると、このメッセージMと共通鍵Ｋとに基づき、ＭＡＣ計算部２３Ｂが第２のＭＡＣ認証子＃２を算出する。

【００５９】

次に、照合部２４Ｂは、この第２のＭＡＣ認証子＃２と受信された第１のＭＡＣ認証子＃１とを比較照合し、両認証子＃１，＃２が一致するときに、第１のエンティティ装置１０Ａにより作成されたメッセージMが改竄されずにメッセージ受信部２１Ｂに受信された旨を認証する。また、照合部２４Ｂは、両認証子＃１，＃２が不一致のときに、第１のエンティティ装置１０Ａにより作成されたメッセージMが改竄された旨を検出する。

【００６０】

このような認証方式において、ＭＡＣ計算部１３Ａ，２３Ｂは、第１の実施形態と同様に、共通鍵Ｋを各鍵データ$Kg2 \sim Kgm$にそれぞれ変換する過程で各変数入力部$V_1 \sim V_{m-1}$から変数$v_1 \sim v_{m-1}$を入力している。従って、前述同様に、メッセージMが各ブロック毎に同一の平文（メッセージ）ブロック$P1 \sim Pm$となっていても、鍵データ$Kg2 \sim Kgm$が互いに異なる値となるので、安全性を向上させることができる。

【００６１】

上述したように本実施形態によれば、認証方式において、ＭＡＣ認証子＃１，＃２を算出する際に、第１の実施形態の暗復号装置を用いたので、第１の実施形態の効果を有する認証方式を実現することができる。

【００６２】

（第４の実施形態）

図６は本発明の第４の実施形態に係る暗号化連鎖方式の適用されたＭＡＣ計算部の構成を示す模式図である。

すなわち、本実施形態は、第３の実施形態の変形例であり、具体的にはＭＡＣ計算部１３Ａ，２３Ｂにおいて、各変数入力部$V_1 \sim V_{m-1}$に代えて、各変換関数$f_1' \sim f_{m-1}'$が、互いに異なる２以上の変換関数のいずれかとして構成さ

れている。なお、図６は前述同様に一方のＭＡＣ計算部１３Ａを例に挙げて示しているが、他方のＭＡＣ計算部２３Ｂも同様の構成となっている。

ここで、互いに異なる変換関数とは、第２の実施形態に述べた通りである。また、各変換関数f_1'～f_{m-1}'に関しても、第２の実施形態に述べた通りである。

以上のような構成としても、第３の実施形態と同様の効果を得ることができる。

【００６３】

なお、上記各実施形態に記載した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【００６４】

ここで、本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【００６５】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施例を実現するための各処理の一部を実行しても良い。

【００６６】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【００６７】

また、記憶媒体は１つに限らず、複数の媒体から本実施例における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【００６８】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施例における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【００６９】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【００７０】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【００７１】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【００７２】

【発明の効果】

以上説明したように本発明によれば、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上し得る暗復号装置、認証装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【図２】

同実施形態における各変数の生成方法の一例を示すフローチャート

【図３】

本発明の第２の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【図４】

本発明の第３の実施形態に係る認証方式の適用された第１及び第２のエンティティ装置の構成を示す模式図

【図５】

同実施形態におけるＭＡＣ計算部の構成を代表して示す模式図

【図６】

本発明の第４の実施形態に係る暗号化連鎖方式の適用されたＭＡＣ計算部の構成を示す模式図

【図７】

従来の暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【符号の説明】

平文ブロックＰ１～Ｐｍ

暗号化関数Ｆ１～Ｆｍ

暗号文ブロックＣ１～Ｃｍ

Ｋ…共通鍵

Ｋｇ２～Ｋｇｍ…鍵データ

$f_1 \sim f_{m-1}$, $f_1' \sim f_{m-1}'$, $g_1 \sim g_{m-1}$…変換関数

$i_1 \sim i_{m-1}$…中間出力

$v_1 \sim v_{m-1}$…変数

$V_1 \sim V_{m-1}$…変数入力部

１０Ａ，２０Ｂ…エンティティ装置

１１Ａ…メッセージ送信部

１２Ａ，２２Ｂ…共通鍵記憶部

１３Ａ，２３Ｂ…ＭＡＣ計算部

１４Ａ…ＭＡＣ送信部

２１Ｂ…メッセージ受信部

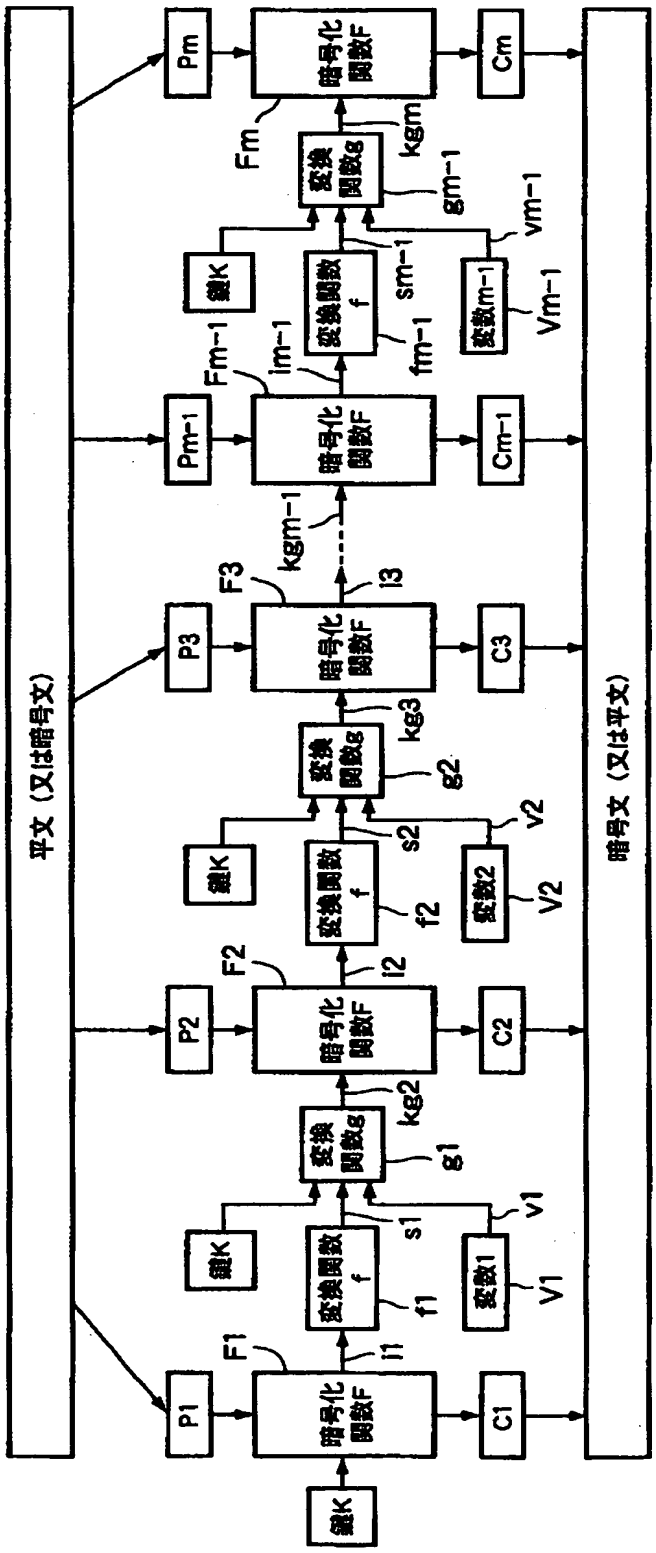
２４Ｂ…照合部

＃１，＃２…ＭＡＣ認証子

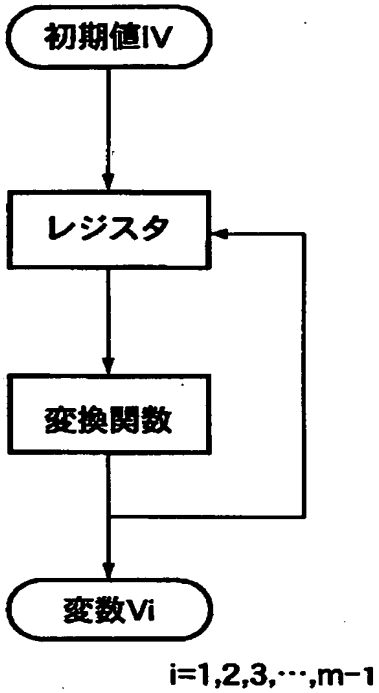
Ｂｓ…ビット選択部

【書類名】　　図面

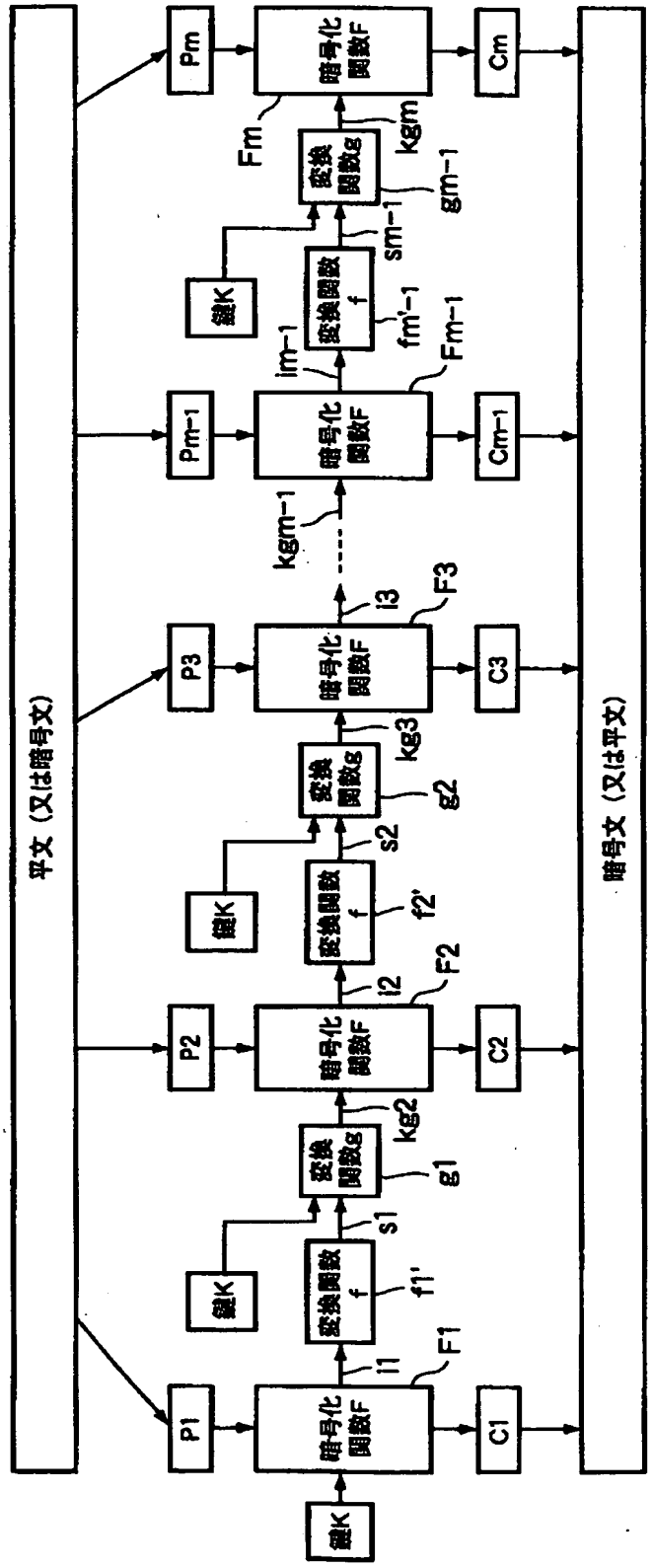
【図１】


平文（又は暗号文）
暗号文（又は平文）
鍵K
P1
暗号化関数F
C1
F1
I1
変換関数f
f1
変数1
V1
s1
v1
変換関数g
g1
kg2
P2
C2
F2
I2
f2
変数2
V2
s2
v2
g2
P3
C3
F3
I3
kg3
Pm-1
Cm-1
Fm-1
Im-1
fm-1
変数m-1
Vm-1
sm-1
vm-1
gm-1
kgm-1
Pm
Cm
Fm
kgm

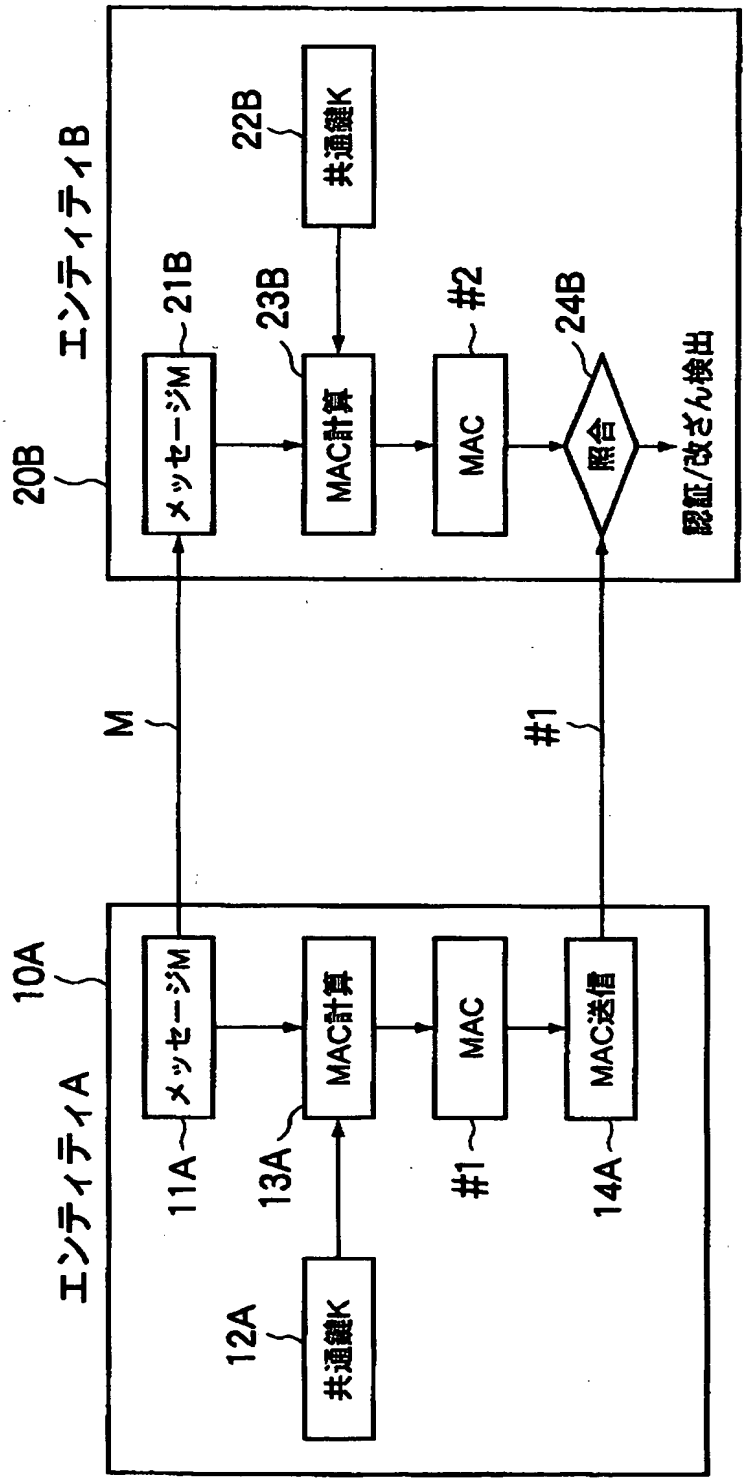
【図２】



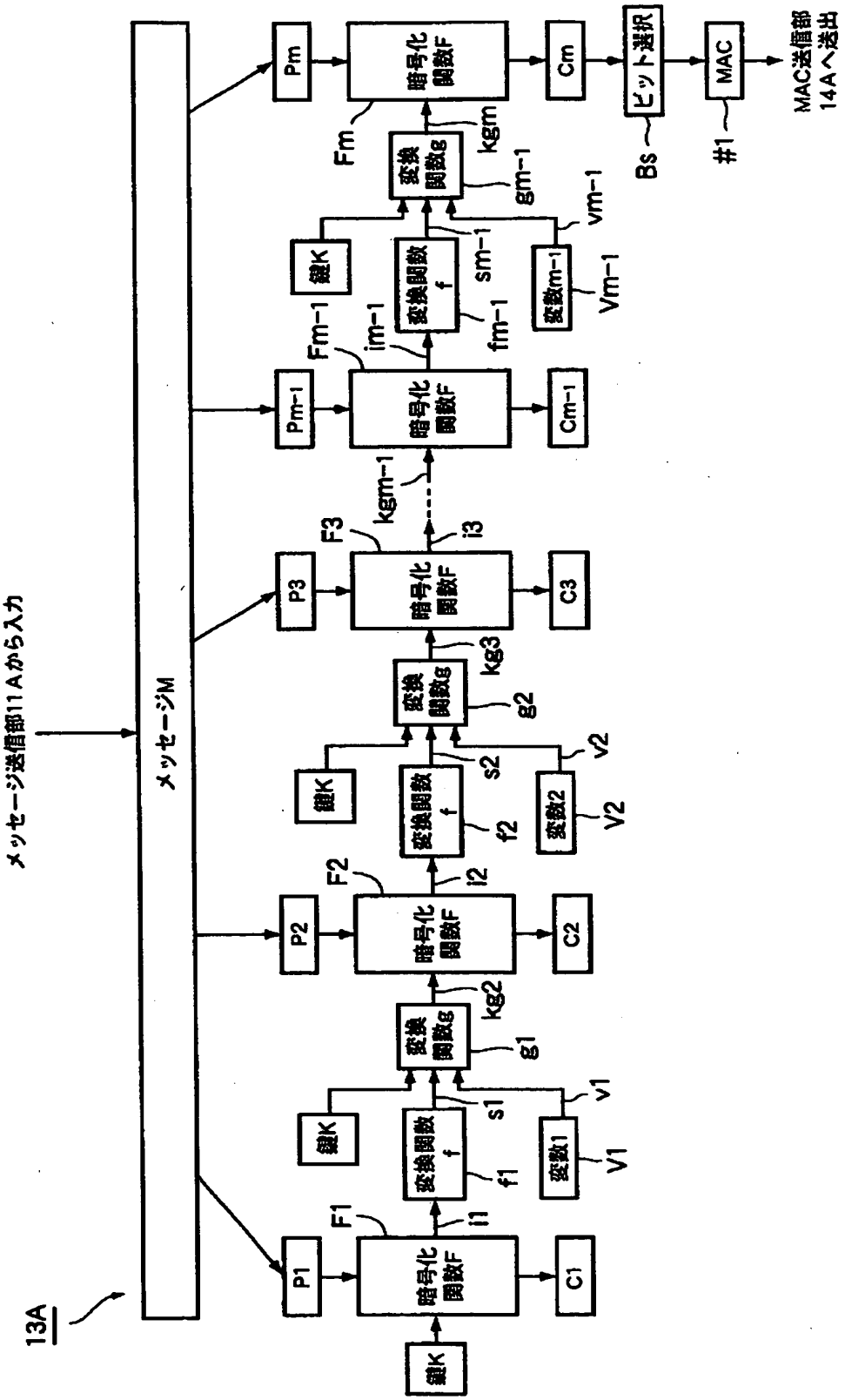
【図３】


平文（又は暗号文）
暗号文（又は平文）
鍵K
暗号化関数F
変換関数f
変換関数g
P1
P2
P3
Pm-1
Pm
C1
C2
C3
Cm-1
Cm
F1
F2
F3
Fm-1
Fm
f1'
f2'
fm'-1
g1
g2
g3
gm-1
gm
i1
i2
i3
im-1
s1
s2
sm-1
kg2
kg3
kgm-1
kgm

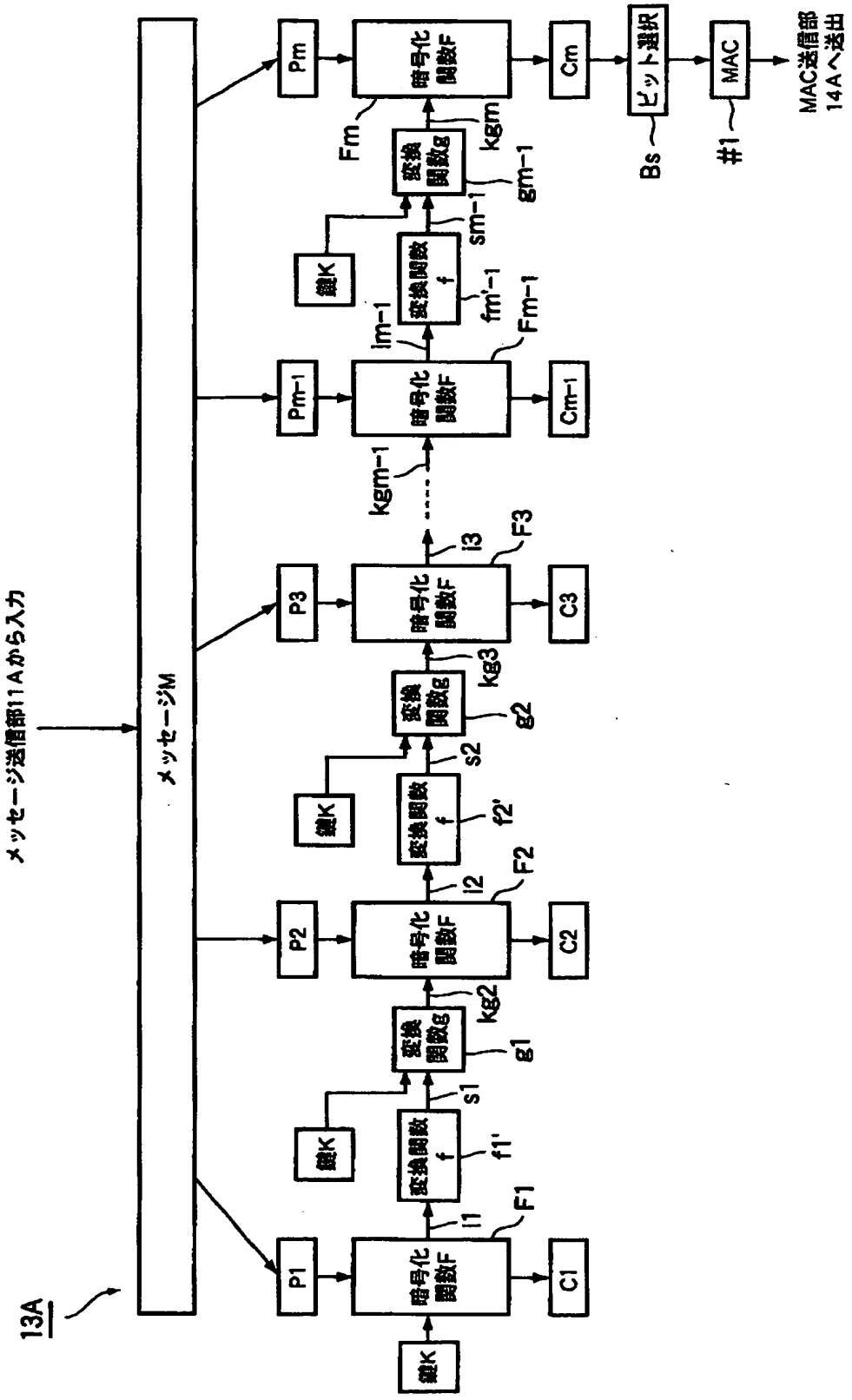
【図４】


エンティティB
20B
メッセージM
21B
MAC計算
23B
共通鍵K
22B
MAC
#2
照合
24B
認証/改ざん検出
M
#1
エンティティA
10A
メッセージM
11A
MAC計算
13A
共通鍵K
12A
MAC
#1
MAC送信
14A

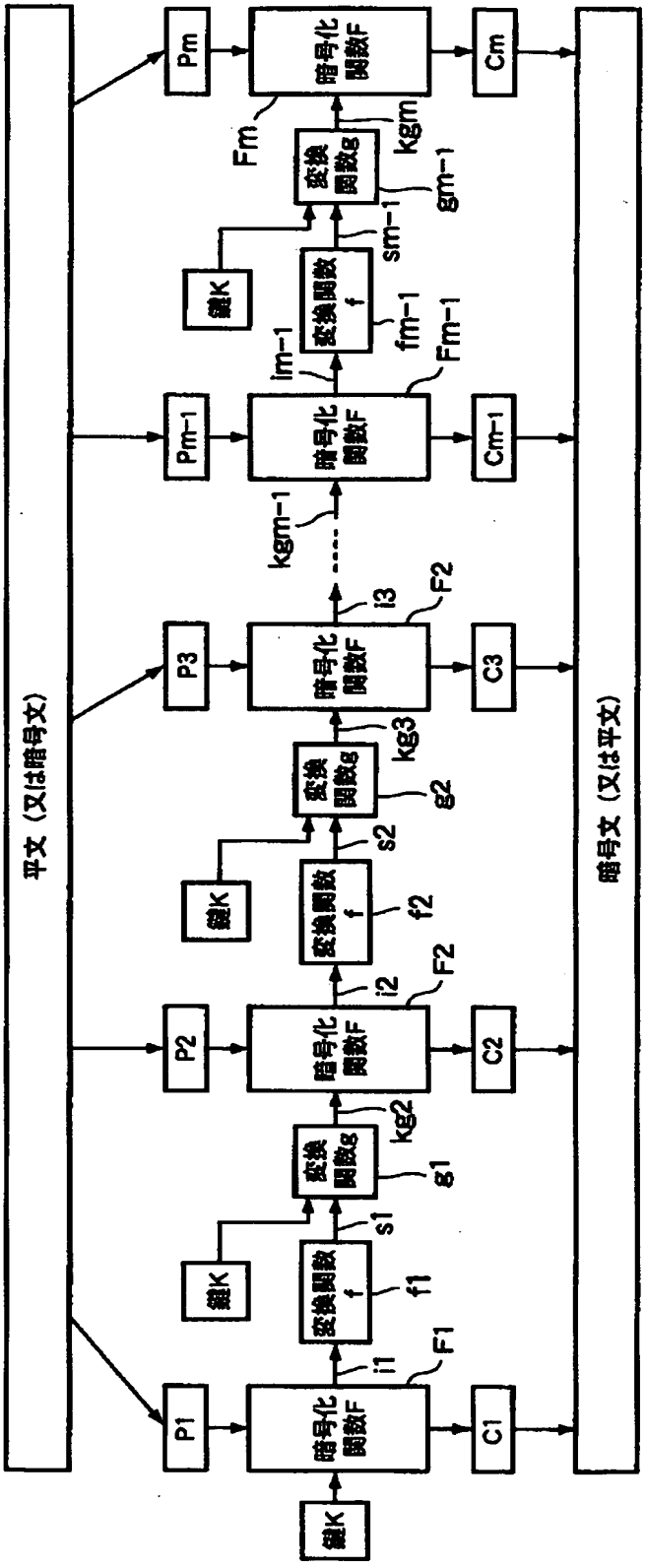
【図５】


メッセージ送信部11Aから入力
メッセージM
13A
鍵K
暗号化関数F
変換関数f
変換関数g
変数1
変数2
変数m-1
ビット選択
MAC
MAC送信部14Aへ送出
P1
P2
P3
Pm-1
Pm
C1
C2
C3
Cm-1
Cm
F1
F2
F3
Fm-1
Fm
i1
i2
i3
im-1
f1
f2
fm-1
g1
g2
gm-1
kg2
kg3
kgm-1
kgm
s1
s2
sm-1
v1
v2
vm-1
V1
V2
Vm-1
Bs
#1

【図６】


メッセージ送信部11Aから入力
メッセージM
13A
P1
P2
P3
Pm-1
Pm
C1
C2
C3
Cm-1
Cm
暗号化関数F
鍵K
変換関数f
変換関数g
F1
F2
F3
Fm-1
Fm
I1
I2
I3
Im-1
f1'
f2'
fm'-1
s1
s2
sm-1
g1
g2
gm-1
kg2
kg3
kgm-1
kgm
ビット選択
Bs
MAC
#1
MAC送信部14Aへ送出

【図７】


平文（又は暗号文）
暗号文（又は平文）
鍵K
暗号化関数F
変換関数f
変換関数g
P1
P2
P3
Pm-1
Pm
C1
C2
C3
Cm-1
Cm
F1
F2
Fm-1
Fm
i1
i2
i3
im-1
f1
f2
s1
s2
sm-1
g1
g2
g3
gm-1
kg2
kg3
kgm-1
kgm

【書類名】　　要約書

【要約】

【課題】　特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させる。

【解決手段】　鍵データＫｇ２～Ｋｇｍは、平文ブロックＰ１～Ｐｍや中間結果i_1～i_{m-1}とは独立に入力される変数v_1～v_{m-1}に基づき、共通鍵Ｋが変換されて作成される。このため、暗復号装置は、平文ブロックＰ１～Ｐｍの各ブロックを互いに同一データとして入力する暗号解読手法に攻撃されても、鍵データＫｇ２～Ｋｇｍを互いに異なる値に作成できる。

【選択図】　図１

出証特２００１－３０６０４９６

出 願 人 履 歴 情 報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝